Mission Possible: How We Defused an In-Progress Identity System Attack

Guido Grillenmeier

Semperis Principal Technologist, EMEA

12 Years Microsoft MVP

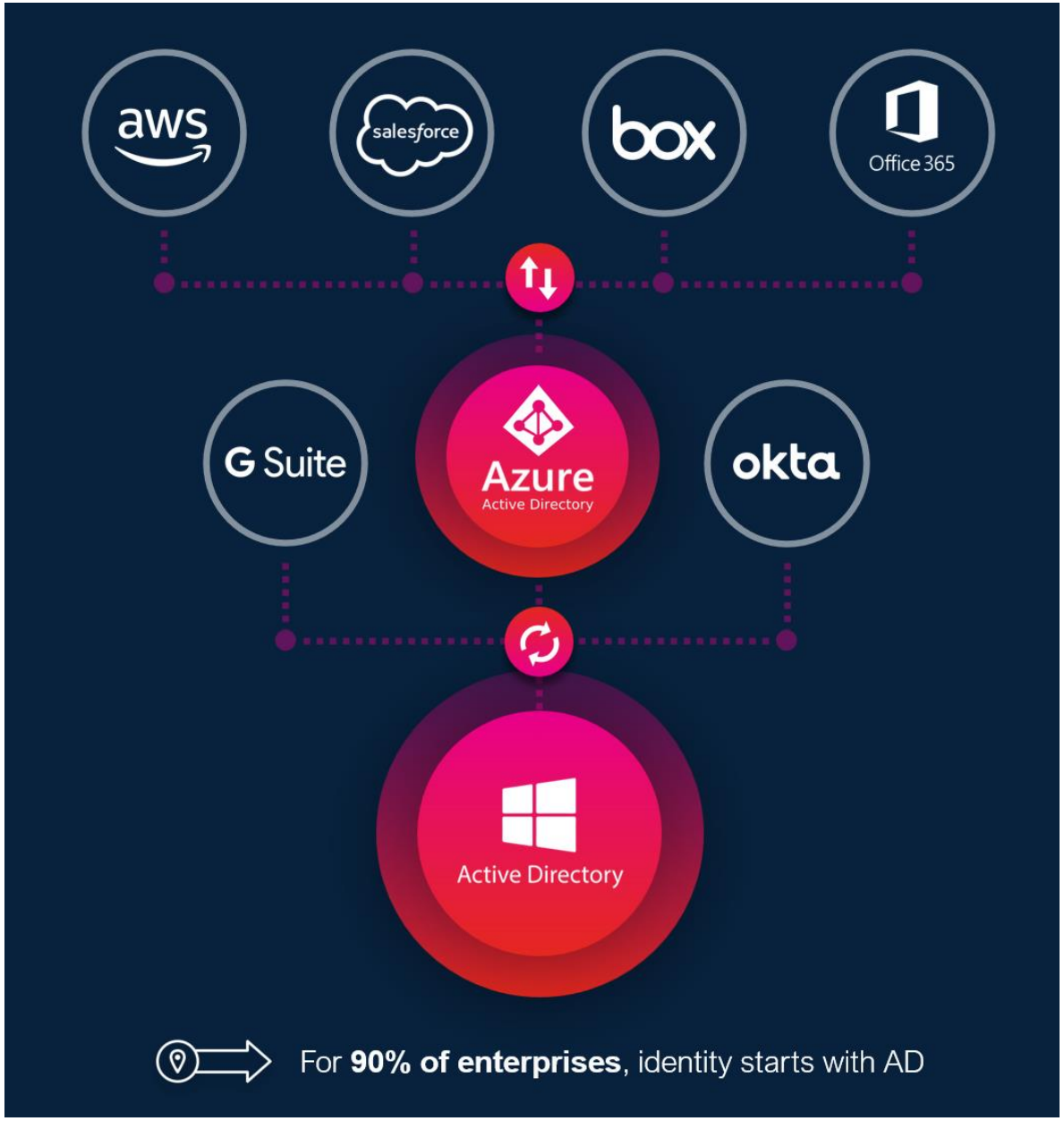
guidog@semperis.com

www.linkedin.com/in/guidogrillenmeier

KEYS TO THE KINGDOM

If Active Directory isn't secure, nothing is

- 90% of all breaches involve credential abuse
- Systemic weakness make AD a soft target
- Cloud identity extends from AD
- Zero trust model assumes hybrid AD integrity



#1 NEW TARGET

90% of attacks investigated involve AD in some form, whether it is the initial attack vector or targeted to achieve persistence or privileges

- Mandiant

Windows 2000: Birth of Active Directory

Windows Server 2003

Gil Kirkpatrick and Guido Grillenmeier publish "A Definitive Guide to Active Directory Disaster Recovery"

Windows Server 2008

- New Windows Server Backup feature
- Volume Shadow Service (VSS) Snapshots of AD
- View previous version of AD
- Protect from accidental deletion
- Read-only domain controllers

Windows Server 2008 R2

Recycle Bin

Windows Server 2012

- UI for Recycle Bin
- VM generation identifier, support for VM snapshots of virtualized DCs
- Direct mounting of VHD files

Windows Server 2012 R2

Security updates such as Protected Users group and authorization policy silos

Windows Server 2016

Mainly security updates, such as shielded VMs and Privileged Access Management (PAM)

Windows Server 2019

No relevant updates to AD

Windows Server 2022

No relevant updates to AD

Phases of a Ransomware-Attack

Initial Access

- Phishing emails
- Malicious websites
- Targeted attacks with **stolen credentials**

BYOVD

Post Exploit

- Download of malware for **Recon-Phase**
- Connection to C2* systems
- Remote connection established

Reconnaissance

- Evaluation of **AD vulnerabilities** to gain domain-dominance
- Lateral movement to other systems
- Credential harvesting and privilege escalation

Core attack

- Access to and Extraction of core-business data
- Encryption of devices, often **including AD DCs**

* C2 = Command-and-Control

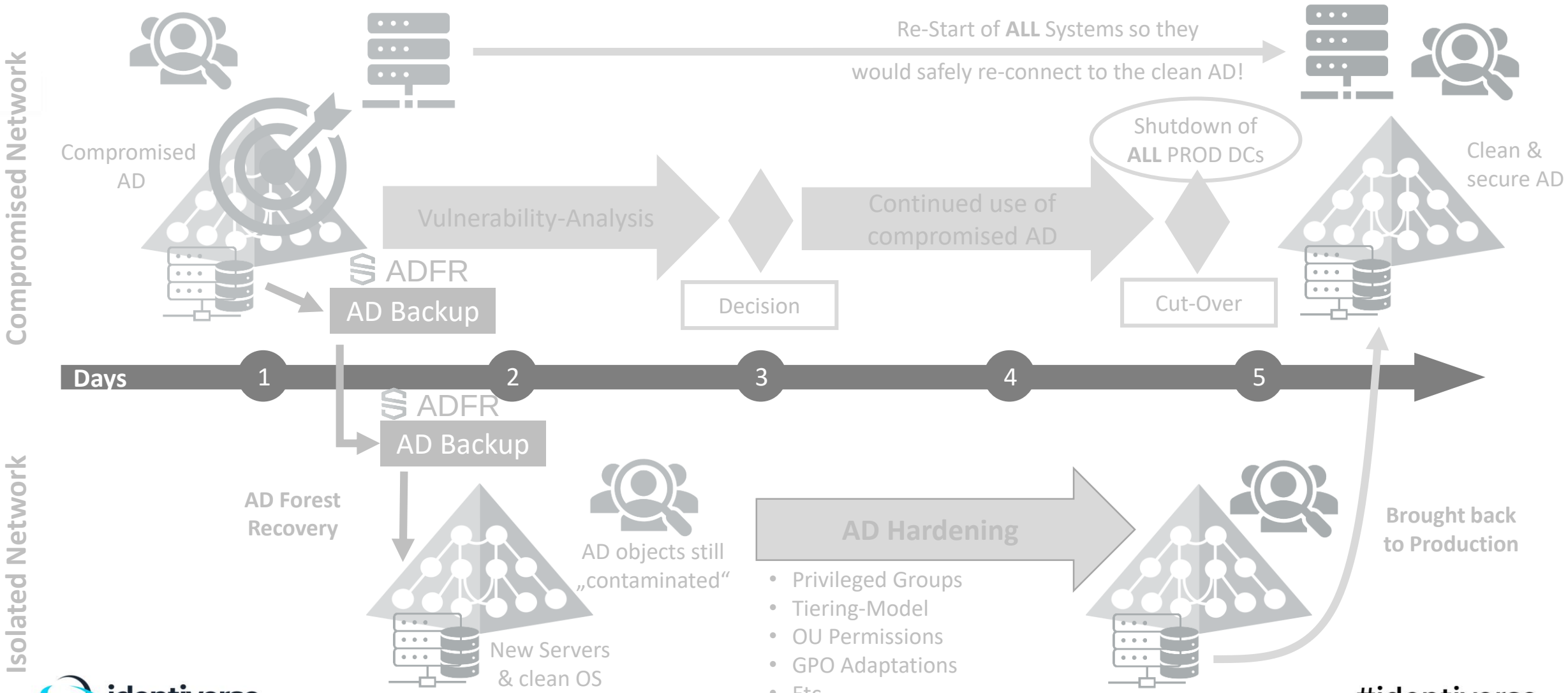
IN → THROUGH → OUT

Sample situation from the trenches

THE VICTIM

- The Middle East
- Important provider of critical infrastructure (Telco & Banking)
- Approx. 1.000 server + many more thousands of OT endpoints
- Partner QGroup from Germany already involved – called Semperis to support with AD IR expertise
- Victim was actively being attacked, but still alive
  ➔ *it was key to keep them alive!*

Real life AD-incident example



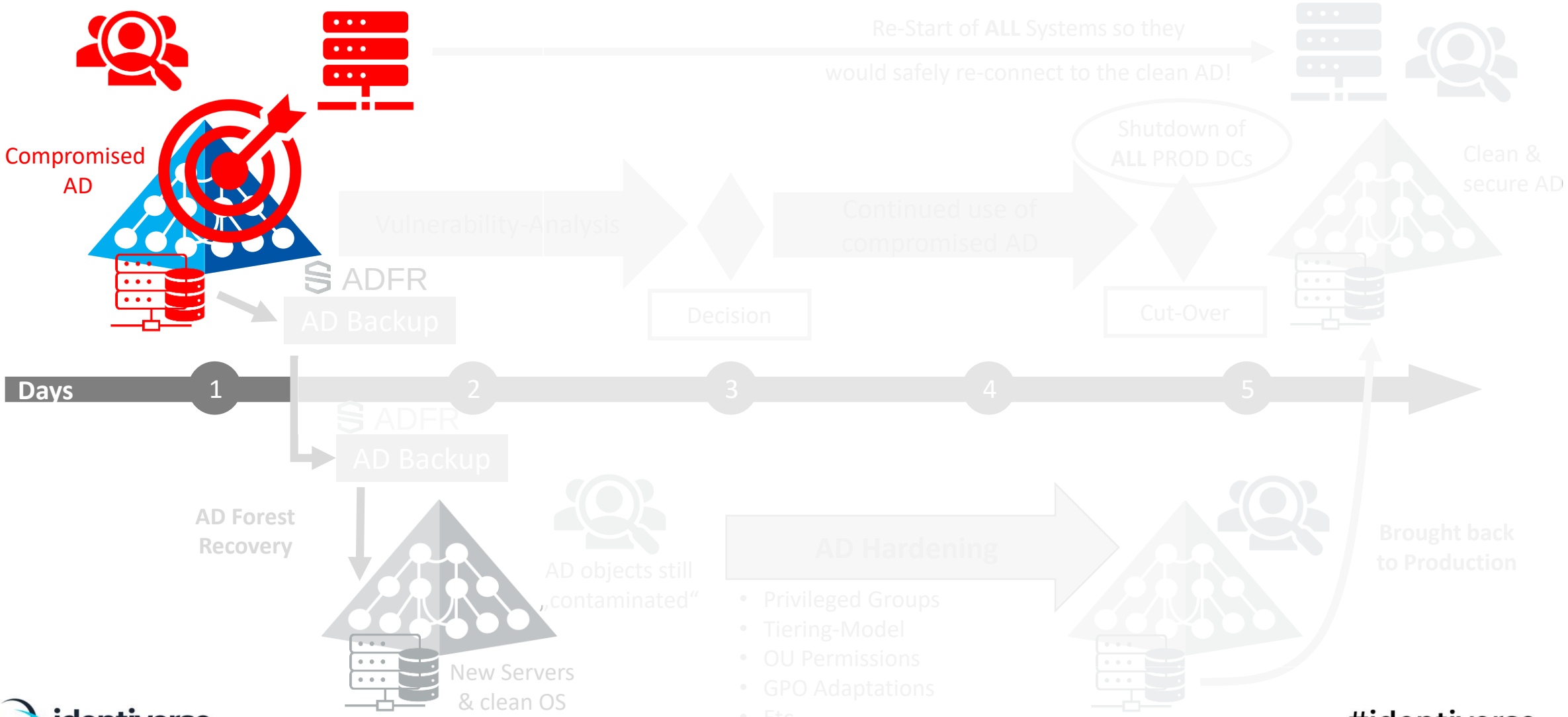
identiverse

#identiverse

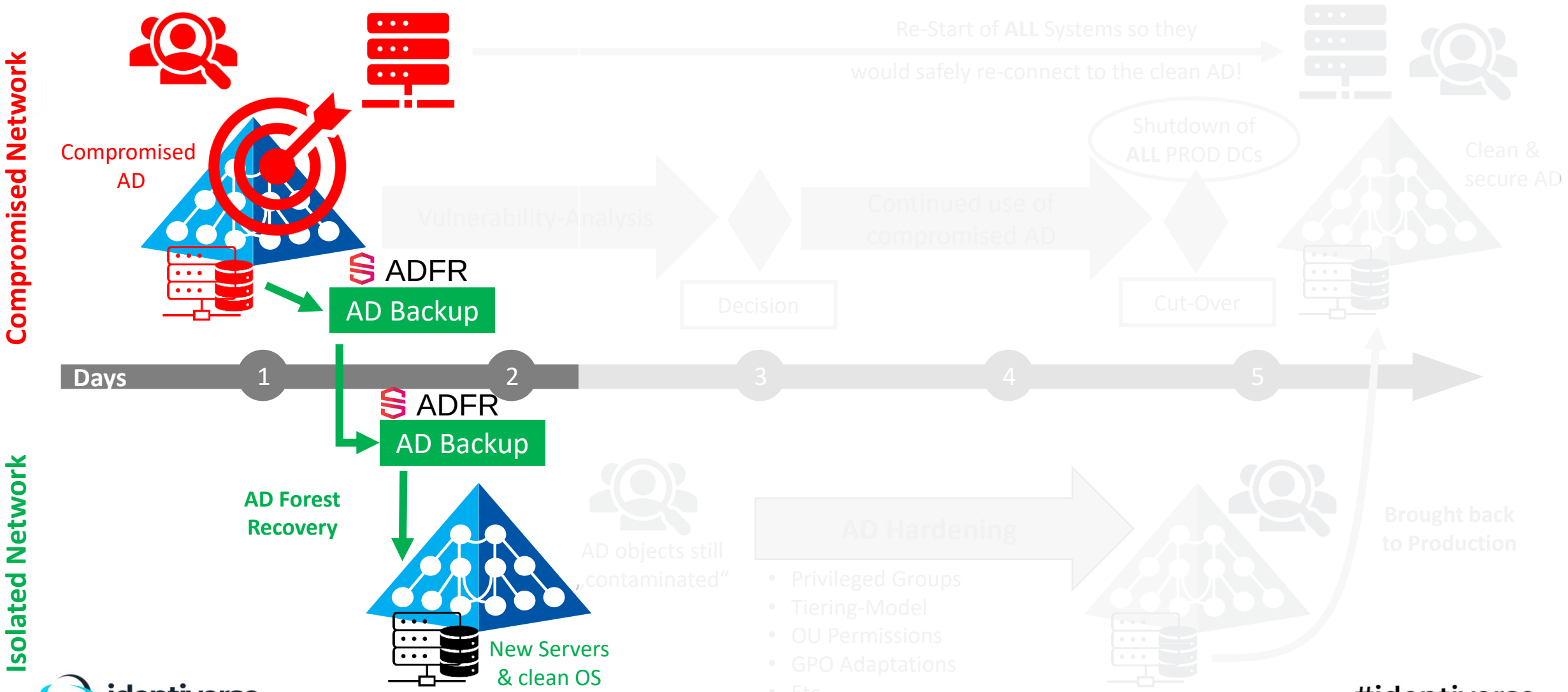
You've been BREACHED !!!

Compromised Network

Isolated Network



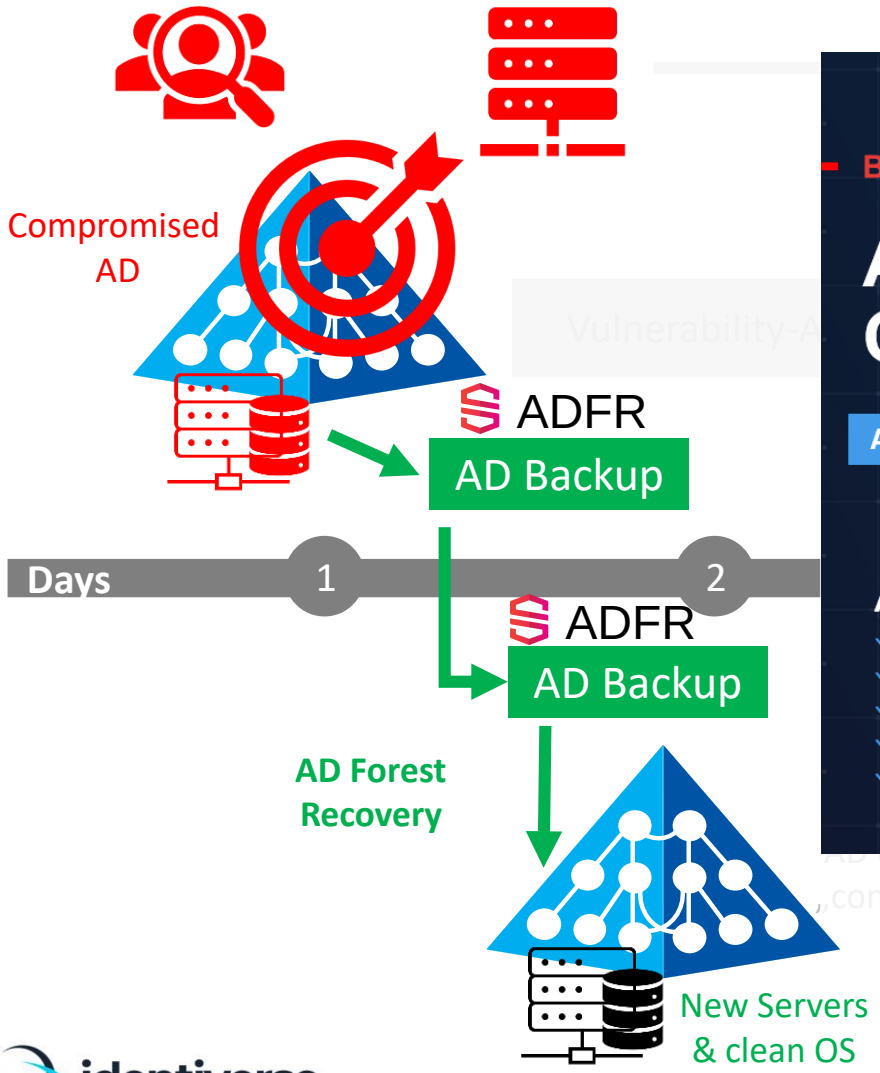
PHASE I – Spin up a SAFETY NET for AD



PHASE I – Spin up a SAFETY NET for AD

Compromised Network

Isolated Network



BACKUP COMPARISON

ADFR vs. other Domain Controller backups

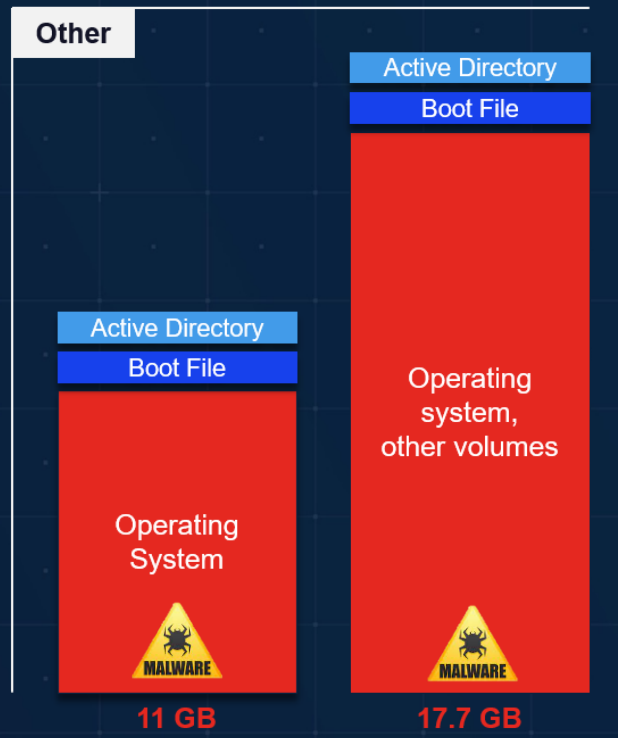
ADFR

116 MB (500 MB uncompressed)

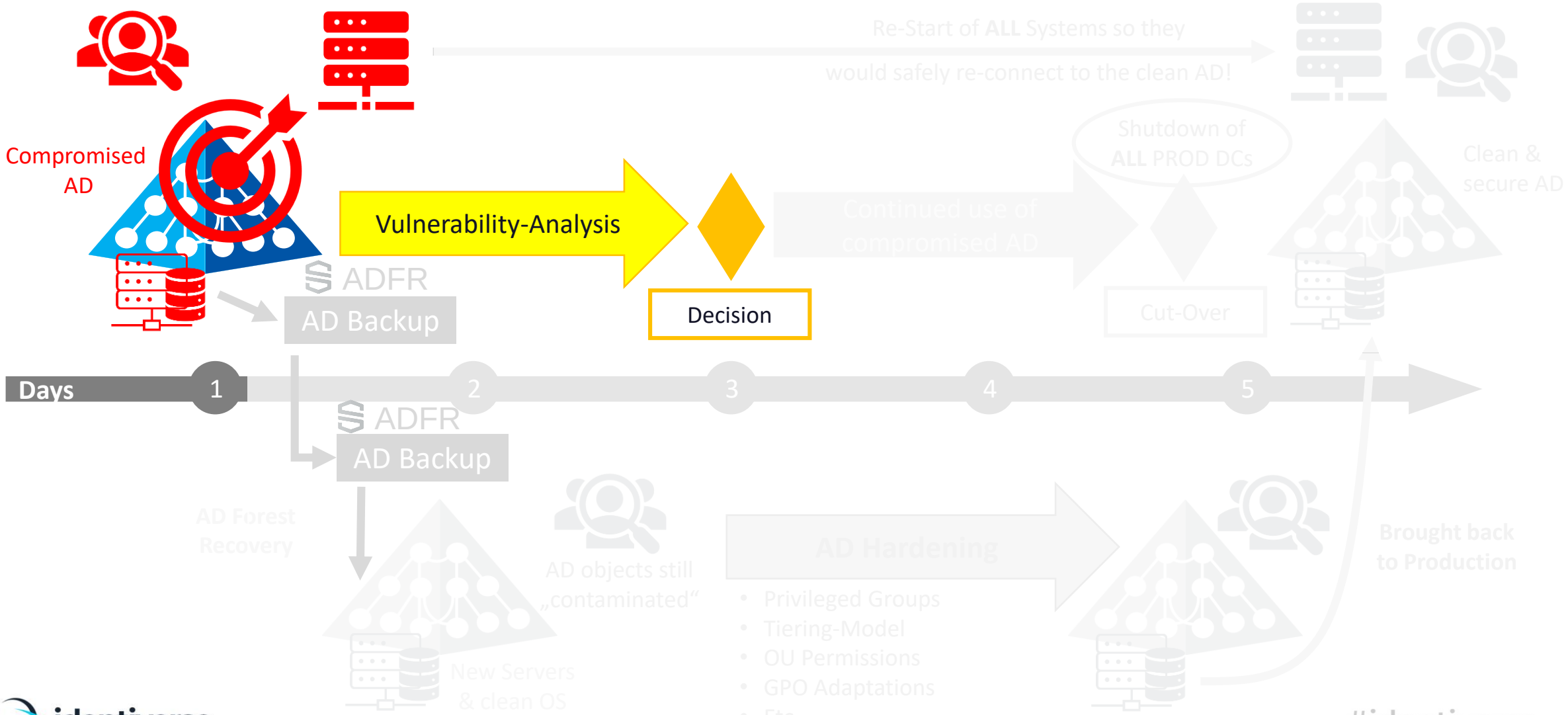
- Active Directory
- Boot File

ADFR backups

- ✓ Contain no OS → no OS-resident malware in recovery
- ✓ Remove dependence on source hardware → recover anywhere
- ✓ Are significantly smaller
- ✓ Provide faster backup and recovery
- ✓ Require less storage



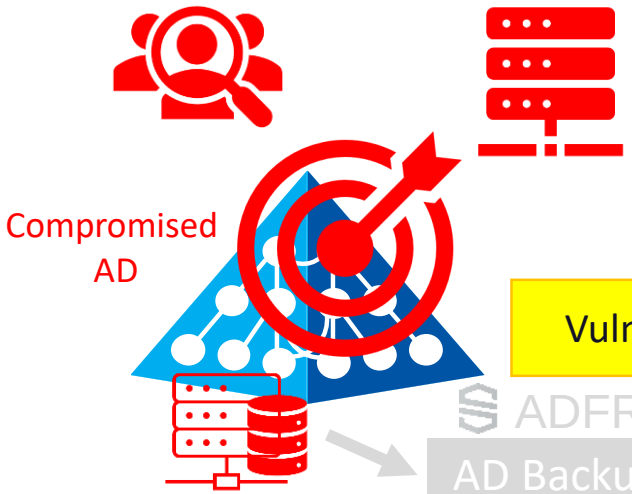
PHASE II – AD Vulnerability Analysis



PHASE II – AD Vulnerability Analysis

Compromised Network

Isolated Network



Vulnerability-Analysis

Decision

ADFR
AD Backup

ADFR
AD Backup

Days 1 2 3

PURPLE KNIGHT

www.purple-knight.com

BLOODHOUND

forest druid
powered by semperis

identiverse

#identiverse

Free AD vulnerability scanning tools

- Requires installation of Java and NeoJ4 DB
- Separate extraction of AD data through additional tool (Sharphound) – which is then processed by BloodHound tool for visualization of attack-path

- Powerful UI tool from Semperis for visualization of attack-path
- Easy to use—no setup required
- Built to help AD defenders

- Command-line tool for evaluating security posture of an AD domain

- Powerful UI-tool from Semperis for evaluating security posture of a complete AD forest
- Continuously updated with new indicators of exposure (IOEs) and indicators of compromise (IOCs)

FREE → www.purple-knight.com
www.purple-knight.com/forest-druid

Dubious permissions & MULTIPLE attackers (!)

SECURITY INDICATOR

Dangerous control paths expose certificate templates

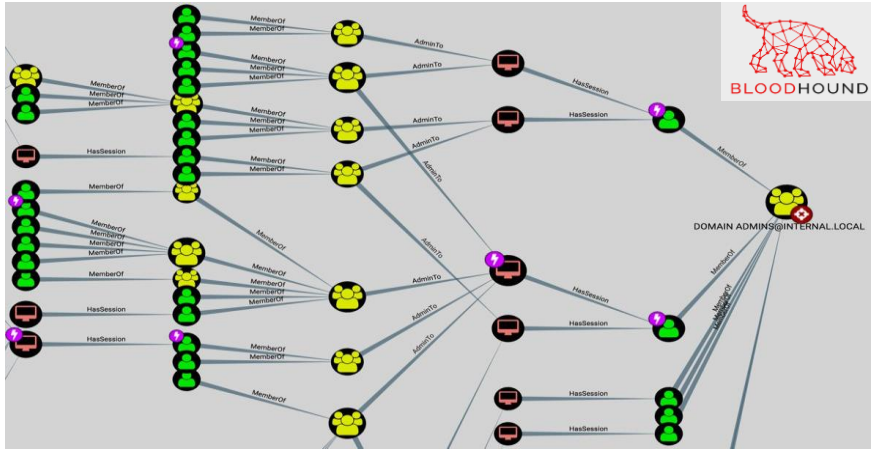
SEVERITY	WEIGHT
Warning	7

Security Frameworks

MITRE ATT&CK

- Credential Access

Domain Computers were allowed to change certificate templates – which allows intruders to create their own authentication certificates for any user!

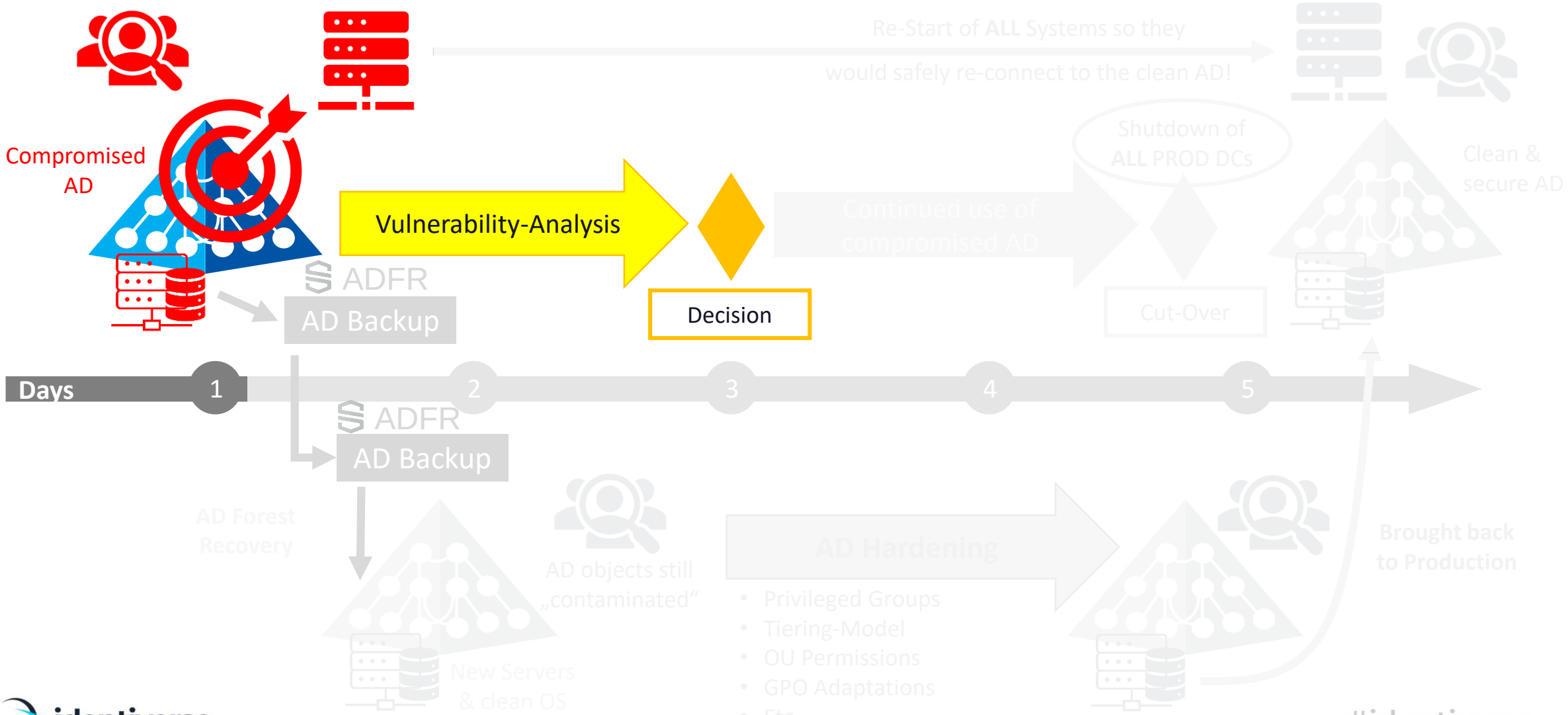


A special **helpdesk account** was granted the rights to **reset the password** of everyone in the domain.

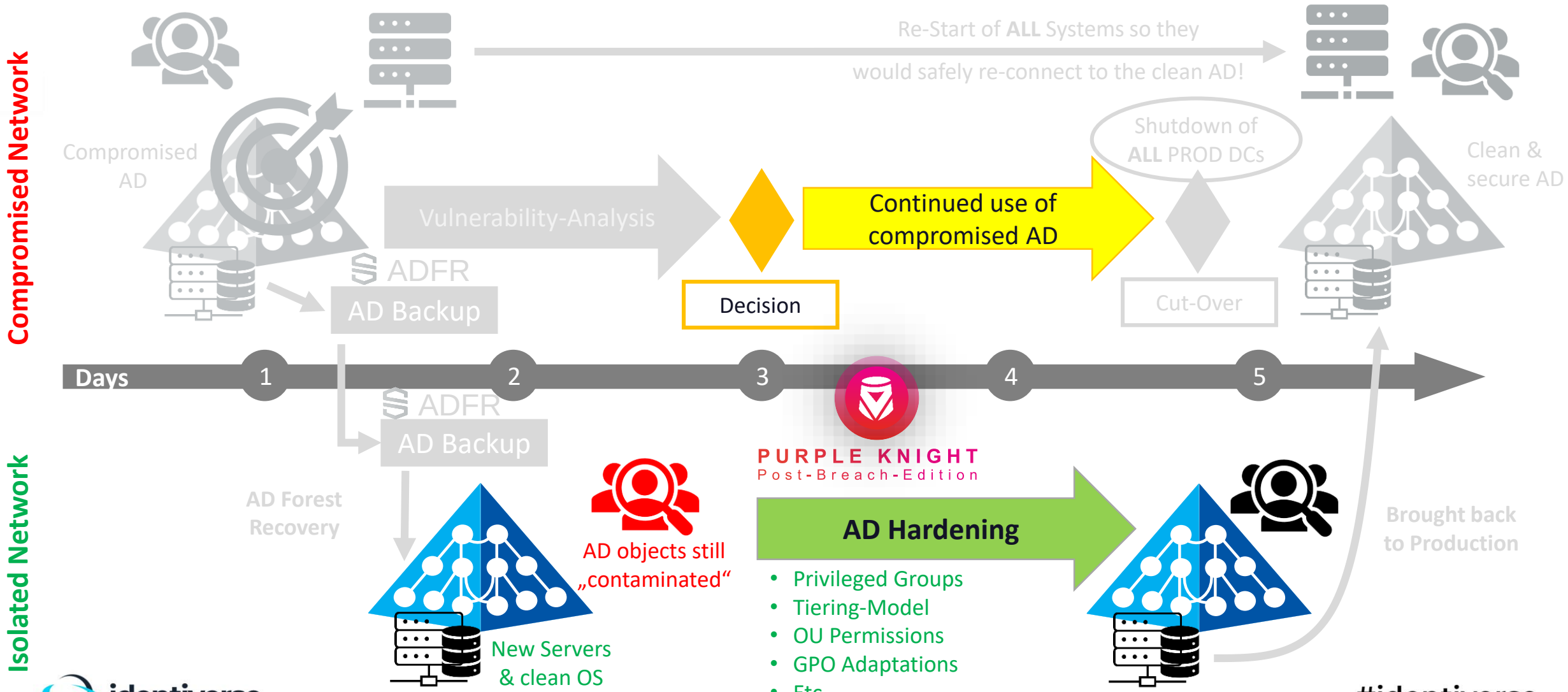
And **EVERYONE** was permissioned to reset the password of the helpdesk account!

Analysis of EDR Team showed that **MULTIPLE attackers were active** in the environment at the SAME time (**four** different “fingerprints” were found) – intruders were happily re-using the existing Domain-Admin accounts whenever one of the AD admins changed their password!

PHASE II – AD Vulnerability Analysis



PHASE III – Divide and Conquer!

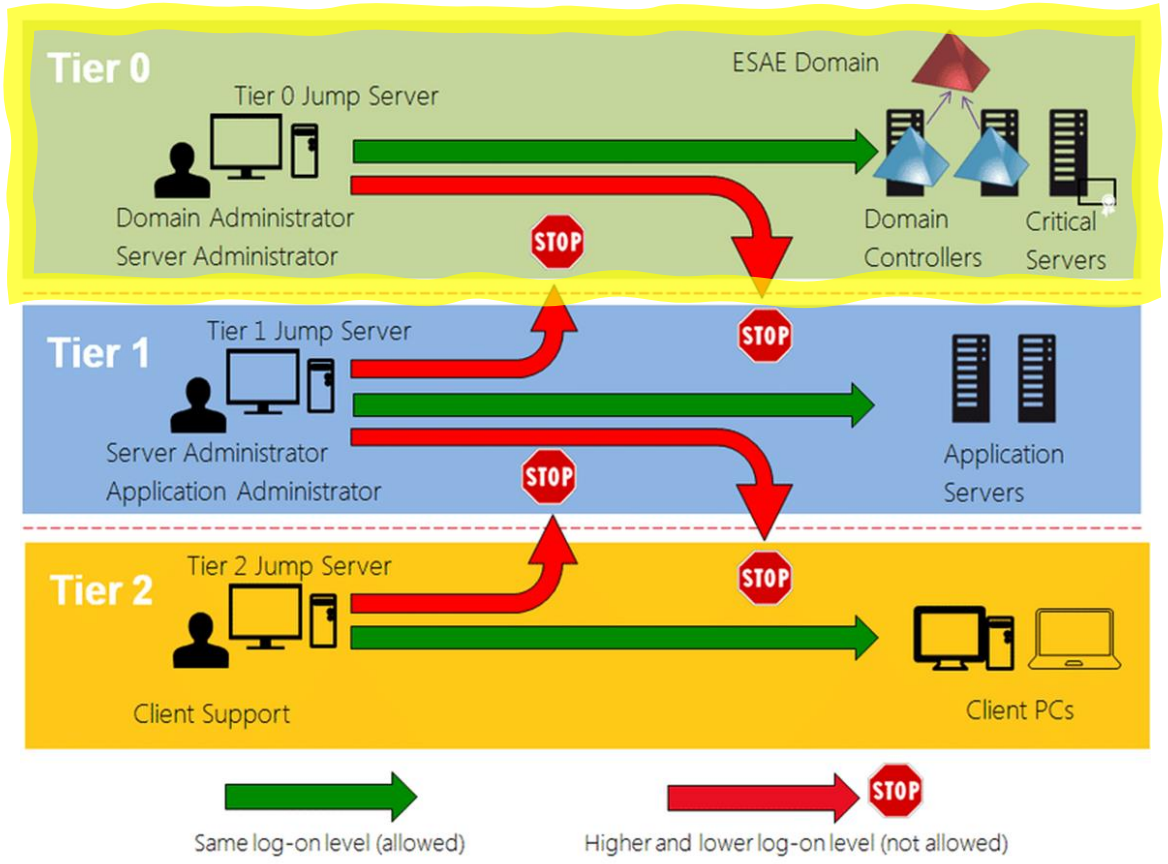


AD Hardening Speedway …

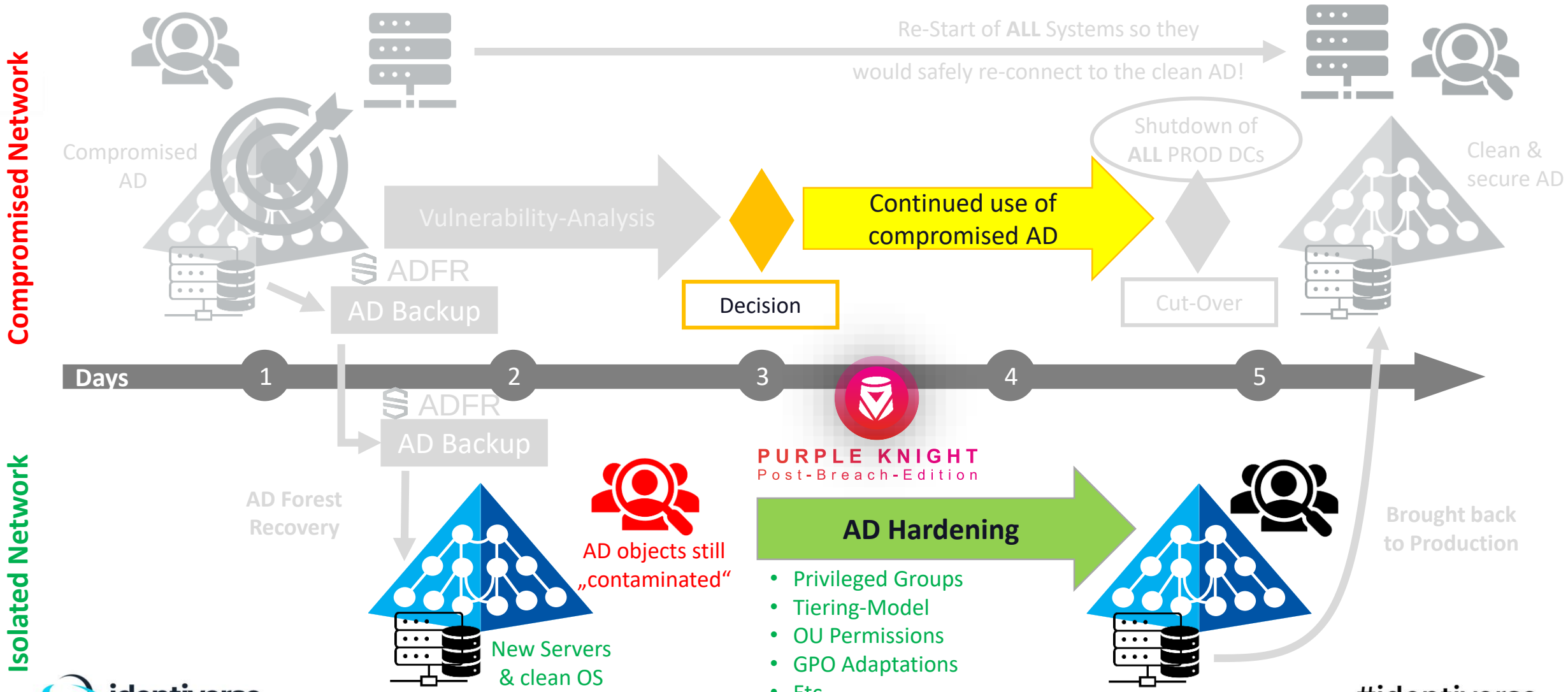
1.5 days available to harden AD

- Tiering-Model (w/o MFA)
- NEW accounts in Privileged Groups
- Protected Users group
- No Privileged Accounts with SPNs
- OU Permissions
- GPO Adaptations
- …

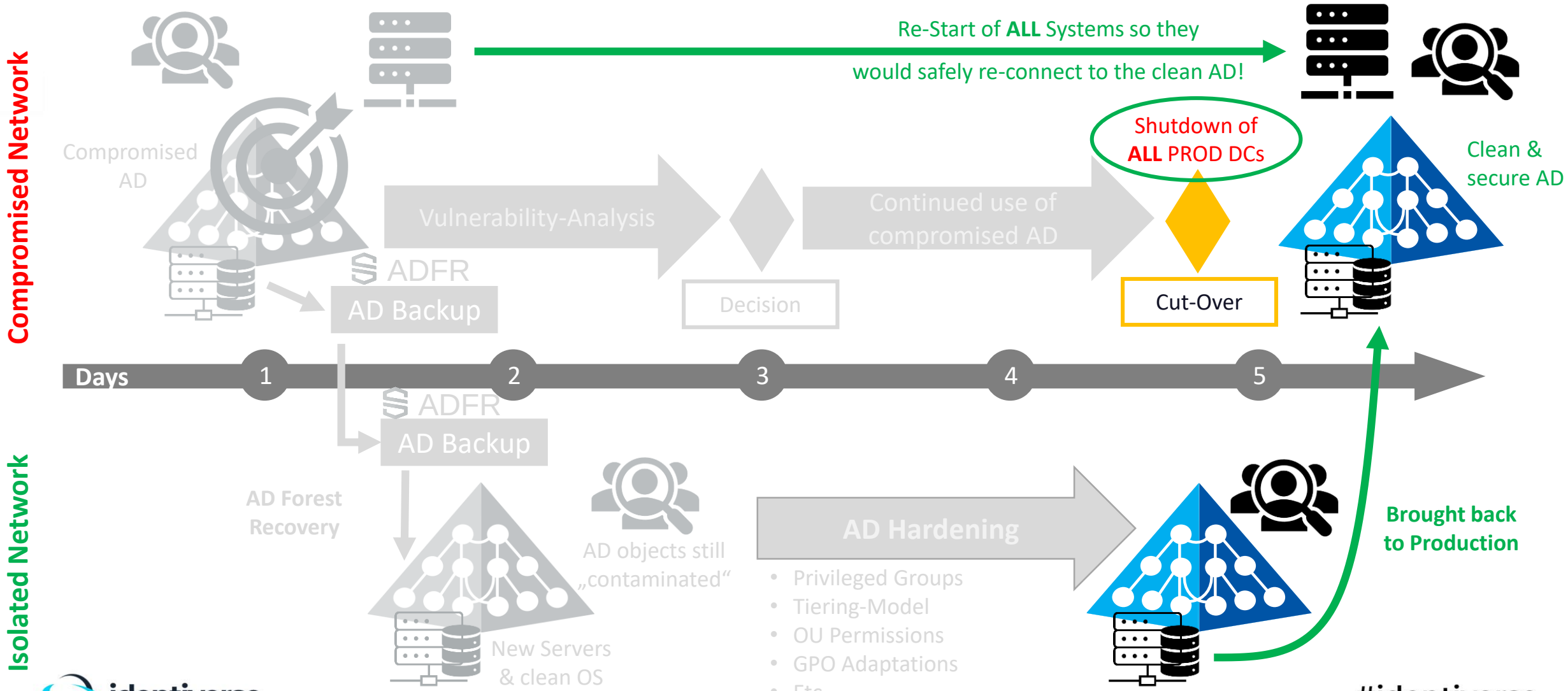
Source: Microsoft



PHASE III – Divide and Conquer!



PHASE IV - Bring hardened AD back to PROD

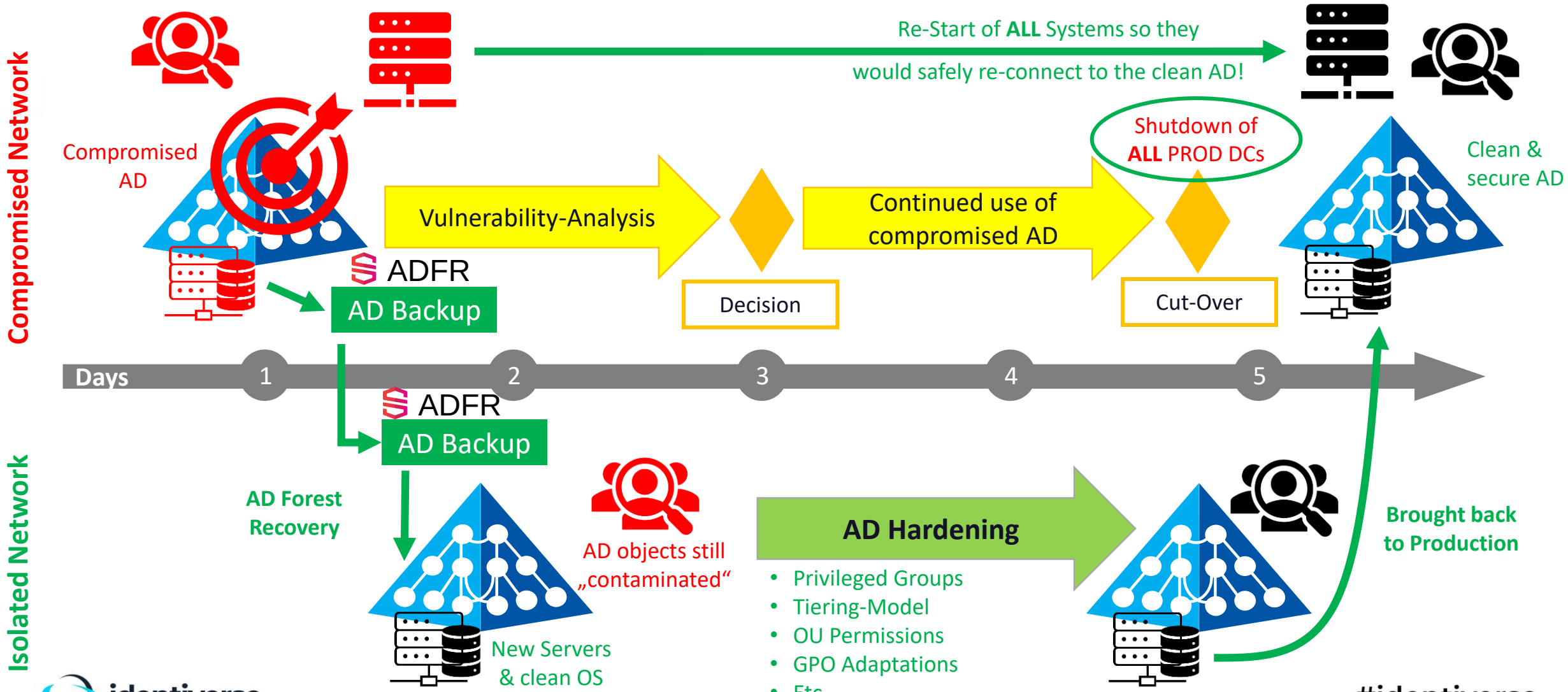


Source: https://www.youtube.com/watch?v=cIpBpGQ0XTI
or search for “changing tires while driving” ☺

Well coordinated efforts to switch recovery AD to PROD

- **Tough decision:** take down ALL existing (compromised) AD DCs of forest in all data-centers
- Change of VLAN and IP-addresses of the recovery AD DCs
  - The AD DCs were also acting as DNS servers …
- Fully working AD was brought back online in all data-centers within **30 min**
- AD Recovery via Semperis ADFR had taken care of many of the tedious prep-steps such as krbtgt password reset
- EDR Team had in parallel taken down more than **20 C2** (!) systems and blocked 100's of external IPs
- **Rebooted all servers** and clients to ensure killing any existing process and to re-create secure channel with recovered AD

Real life AD-incident example - they SURVIVED!



identiverse

#identiverse

Key Outcome

1. Very FAST recovery of a fully functional and SAFE Active Directory
2. NO more pwned privileged accounts ava[illegible]ymore for the attackers to leverage!
3. All existing Apps even inc[illegible]AD pass-through authentication for C[illegible]tinued to work seamlessly after recovery

Semperis helped them to survive!

Thank you!

Questions?
Get in touch …

Guido Grillenmeier

Principal Technologist, EMEA
SEMPERIS

guidog@semperis.com
www.linkedin.com/in/guidogrillenmeier